PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-030138
(43)Date of publication of application : 31.01.2003

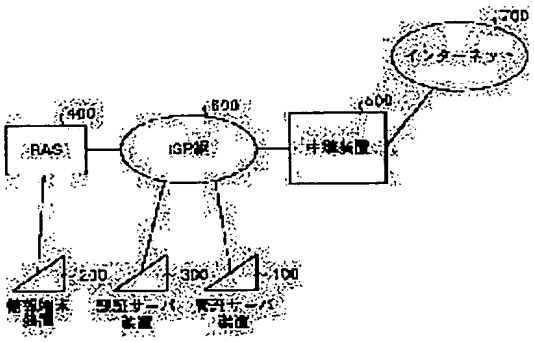
(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 12/46
H04L 12/66

(21)Application number : 2001-211165
(22)Date of filing : 11.07.2001

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : NAGASHIMA NORIMITSU
ATOZAWA SHINOBU

(54) INTERNET CONNECTION SYSTEM, MANAGING SEVER DEVICE, INTERNET CONNECTING METHOD, AND PROGRAM MAKING COMPUTER IMPLEMENT THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide safe Internet connection service for a user who does not have security knowledge without introducing implements and materials such as a firewall into individual users.
SOLUTION: An information terminal device 200 is connected to an ISP(Internet service provider) network 600 through a RAS(remote access server) 400. RAS 400 receives a connection request from the information terminal device 200 of a user and relays data to the ISP network 600. The ISP network 600 includes an authentication server device 300 which checks a user ID and a password and a managing server device 100 which manages information on contracting users. The managing server device 100 stores user information on application kinds, data directions, etc., that the user applied when making a contract.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－30138
（Ｐ２００３－３０１３８Ａ）
(43)公開日　平成15年１月31日(2003.1.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 15/00	310	G06F 15/00	310	D 5B085
13/00	351	13/00	351	Z 5B089
H04L 12/46		H04L 12/46		E 5K030
12/66		12/66		B 5K033

審査請求　未請求　請求項の数18　ＯＬ　（全17頁）

(21)出願番号　特願2001－211165(Ｐ2001－211165)

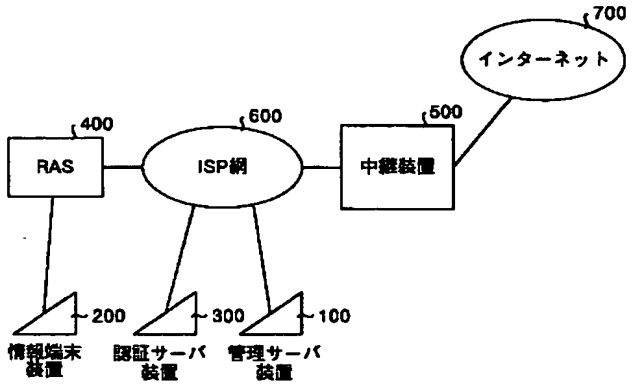
(22)出願日　平成13年７月11日(2001.7.11)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　永嶋　規充
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　後沢　忍
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】インターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラム

(57)【要約】
【課題】　ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供すること。
【解決手段】　情報端末装置２００は、ＲＡＳ４００を介してＩＳＰ網６００に接続される。ＲＡＳ４００は、ユーザの情報端末装置２００からの接続要求を受け、データをＩＳＰ網６００に中継する。ＩＳＰ網６００には、ユーザＩＤ、パスワードをチェックする認証サーバ装置３００、契約したユーザの情報を管理する管理サーバ装置１００を含んで構成される。管理サーバ装置１００には、ユーザが契約時に申請したアプリケーション種別やデータ方向等のユーザ情報が格納されている。



1

【特許請求の範囲】

【請求項１】　ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムにおいて、

前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、

前記ユーザに対してユーザＩＤおよびパスワードを発行する発行手段と、

前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザＩＤおよび前記パスワードを受信し、当該ユーザＩＤおよび当該パスワードが前記発行手段によって前記ユーザに発行されたものであるか否かを認証する認証手段と、

前記認証手段によって認証された場合には、前記ユーザの前記情報端末装置に対してＩＰアドレスを割り当てるＩＰ割当手段と、

前記ユーザが送受信する前記データが前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定手段と、

を備え、前記条件判定手段によって合致すると判定された前記データについて送受信を許可することを特徴とするインターネット接続システム。

【請求項２】　前記ユーザが前記インターネットの接続を切断した場合には、前記ＩＰ割当手段によって割り当てた前記ＩＰアドレスを無効にするＩＰアドレス無効手段をさらに備えたことを特徴とする請求項１に記載のインターネット接続システム。

【請求項３】　前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更手段、

をさらに備えたことを特徴とする請求項１または２に記載のインターネット接続システム。

【請求項４】　前記条件判定手段によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信手段、

をさらに備えたことを特徴とする請求項１～３のいずれか一つに記載のインターネット接続システム。

【請求項５】　前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、

前記条件判定手段は、前記ユーザが送受信する前記データが前記契約登録手段にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、

2

前記条件判定手段によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする請求項１～４のいずれか一つに記載のインターネット接続システム。

【請求項６】　前記契約変更手段は、

登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、

登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段と、

をさらに備えたことを特徴とする請求項３～５のいずれか一つに記載のインターネット接続システム。

【請求項７】　ユーザの認証を行う認証サーバと、インターネットに接続された中継装置とを通信可能に接続して構成された、前記ユーザの情報端末装置を前記インターネットに接続するインターネット接続システムの管理サーバ装置において、

前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、

前記ユーザに対してユーザＩＤおよびパスワードを発行する発行手段と、

前記認証サーバにおいて前記ユーザＩＤおよび前記パスワードが認証され、ＩＰアドレスを割り当てられた前記ユーザに対して、当該ＩＰアドレスと、前記アプリケーション種別情報と、前記データ方向情報とを対応付けて格納するユーザ情報格納手段と、

前記ユーザ情報格納手段によって格納された当該ＩＰアドレスと、前記アプリケーション種別情報と、前記データ方向情報とを前記中継装置に対して送信するユーザ情報送信手段と、

を備え、前記中継装置において、前記ユーザが送受信する前記データが前記アプリケーション種別情報および前記データ方向情報に合致するか否かを判定し、合致すると判定された前記データについて送受信を許可することを特徴とする管理サーバ装置。

【請求項８】　前記ユーザが前記インターネットの接続を切断した場合には、割り当てられた前記ＩＰアドレスを無効にするＩＰアドレス無効手段をさらに備えたことを特徴とする請求項７に記載の管理サーバ装置。

【請求項９】　前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更手段、

をさらに備えたことを特徴とする請求項７または８に記載の管理サーバ装置。

【請求項１０】　前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を

拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、
前記ユーザ情報格納手段は、前記ユーザの当該ＩＰアドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とをさらに対応付けて格納し、
前記ユーザ情報送信手段は、前記ユーザの当該ＩＰアドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とを前記中継装置に対してさらに送信し、
前記中継装置において、前記ユーザが送受信する前記データが前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、合致すると判定した場合には、当該データを廃棄することを特徴とする請求項７～９のいずれか一つに記載の管理サーバ装置。
【請求項１１】　前記契約変更手段は、
登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、
登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段と、
をさらに備えたことを特徴とする請求項９または１０に記載の管理サーバ装置。
【請求項１２】　ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムにおいて実行されるインターネット接続方法において、
前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録工程と、
前記ユーザに対してユーザＩＤおよびパスワードを発行する発行工程と、
前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザＩＤおよび前記パスワードを受信し、当該ユーザＩＤおよび当該パスワードが前記発行工程によって前記ユーザに発行されたものであるか否かを認証する認証工程と、
前記認証工程によって認証された場合には、前記ユーザの前記情報端末装置に対してＩＰアドレスを割り当てるＩＰ割当工程と、
前記ユーザが送受信する前記データが前記契約登録工程によって登録されたアプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定工程と、
を含み、前記条件判定工程によって合致すると判定された前記データについて送受信を許可することを特徴とするインターネット接続方法。
【請求項１３】　前記ユーザが前記インターネットの接続を切断した場合には、前記ＩＰ割当工程によって割り当てた前記ＩＰアドレスを無効にするＩＰアドレス無効工程をさらに含むことを特徴とする請求項１２に記載のインターネット接続方法。
【請求項１４】　前記契約登録工程によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更工程、
をさらに含むことを特徴とする請求項１２または１３に記載のインターネット接続方法。
【請求項１５】　前記条件判定工程によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信工程、
をさらに含むことを特徴とする請求項１２～１４のいずれか一つに記載のインターネット接続方法。
【請求項１６】　前記契約登録工程は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、
前記条件判定工程は、前記ユーザが送受信する前記データが前記契約登録工程にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、
前記条件判定工程によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする請求項１２～１５のいずれか一つに記載のインターネット接続方法。
【請求項１７】　前記契約変更工程は、
登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更工程と、
登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更工程と、
をさらに含むことを特徴とする請求項１４～１６のいずれか一つに記載のインターネット接続方法。
【請求項１８】　請求項１２～１７のいずれか一つに記載されたインターネット接続方法をコンピュータに実行させるプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、ユーザの安全性を高めることができるインターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラムに関するものである。
【０００２】
【従来の技術】インターネットの普及に伴い、会社や家庭からネットワークサービスを利用するユーザが増えている。また、近年、ＡＤＳＬ（Ａｓｙｎｃｈｒｏｎｏｕｓ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎ

ｅ）、光ファイバなどの高速、広帯域ネットワーク技術の発展により、ユーザの利用形態はインターネットを利用する時だけ接続するダイヤルアップ接続から常時接続へと変化してきている。

【０００３】ここで、インターネットを常時接続で使用する場合には、使用するアドレスが固定的になるため、接続の度に割り付けアドレスが変わるダイヤルアップ接続に比べ、悪意のあるユーザ（クラッカー）によるインターネットからの不正アクセスの危険性が高くなる問題がある。そのため、ユーザは、ファイアウォールなどの機器を導入し、不正アクセスに対処するケースが多く見られる。

【０００４】図１０は、文献「ＯＰＥＮＤＥＳＩＧＮ Ｎｏ．１４」第８頁（ＣＱ出版社ＩＳＢＮ４－７８９８－１８０８－３）に記載されているファイアウォールが接続されたネットワーク構成図である。

【０００５】図１０において、組織ネットワーク６３は、複数の組織内ネットワーク１、２、３（６０、６１、６２）から構成される。組織ネットワーク６３は、ルータ６４を介してインターネット６５に接続されている。ルータ６４は、組織ネットワーク６３からインターネット６５への接続部分を１箇所に制限し、通過するデータのフィルタリングを行うことでファイアウォールとして動作し、組織ネットワーク６３の安全性を保っている。

【０００６】ここで、家庭からのインターネット接続における一般的なケースを一例として説明すると、端末６７は、モデムを用いてインターネット接続サービスを提供するＩＳＰ（Ｉｎｔｅｒｎｅｔ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）６６にダイヤルアップして、インターネット６５に接続する。

【０００７】

【発明が解決しようとする課題】しかしながら、このようなケースでは、家庭の端末６７には多くの場合フィルタリングを行うファイアウォールは存在せず、インターネット６５とユーザの端末６７との間の通信データはすべて許可されることになる。そのため、インターネット６５から端末６７への不正アクセスや、端末６７からインターネット６５への不用意なデータ流出の可能性がある。従って、上述した従来の方法では、不正アクセスを防止するためには、ユーザ個々にファイアウォールを導入する必要があるという問題がある。

【０００８】また、ユーザが、導入したファイアウォールのルール設定を誤ることによりセキュリティが低下する恐れもあるため、ファイアウォールを導入する際にはネットワークやセキュリティに関する高度な知識がユーザに要求されるという問題がある。

【０００９】この発明は上記に鑑みてなされたもので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができるインターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラムを得ることを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するため、この発明にかかるインターネット接続システムは、ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムにおいて、前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、前記ユーザに対してユーザＩＤおよびパスワードを発行する発行手段と、前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザＩＤおよび前記パスワードを受信し、当該ユーザＩＤおよび当該パスワードが前記発行手段によって前記ユーザに発行されたものであるか否かを認証する認証手段と、前記認証手段によって認証された場合には、前記ユーザの前記情報端末装置に対してＩＰアドレスを割り当てるＩＰ割当手段と、前記ユーザが送受信する前記データが前記契約登録手段によって登録されたアプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定手段とを備え、前記条件判定手段によって合致すると判定された前記データについて送受信を許可することを特徴とする。

【００１１】この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザＩＤおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザＩＤおよびパスワードを受信し、ユーザＩＤおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に対してＩＰアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をＩＳＰ等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【００１２】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記ユーザが前記インターネットの接続を切断した場合には、前記ＩＰ割当手

段によって割り当てた前記ＩＰアドレスを無効にするＩＰアドレス無効手段をさらに備えたことを特徴とする。

【００１３】この発明によれば、ユーザがインターネットの接続を切断した場合には、ＩＰ割当手段によって割り当てた前記ＩＰアドレスを無効にするので、ＩＳＰ等に設定されたユーザの情報を削除することができるようになる。

【００１４】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記契約登録手段によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更手段をさらに備えたことを特徴とする。

【００１５】この発明によれば、登録されたアプリケーション種別情報およびデータ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【００１６】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記条件判定手段によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信手段をさらに備えたことを特徴とする。

【００１７】この発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【００１８】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、前記条件判定手段は、前記ユーザが送受信する前記データが前記契約登録手段にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、前記条件判定手段によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする。

【００１９】この発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めＩＳＰ等に登録することができるようになる。

【００２０】つぎの発明にかかるインターネット接続システムは、上記の発明において、前記契約変更手段は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段とをさらに備えたことを特徴とする。

【００２１】この発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【００２２】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、ユーザの認証を行う認証サーバと、インターネットに接続された中継装置とを通信可能に接続して構成された、前記ユーザの情報端末装置を前記インターネットに接続するインターネット接続システムの管理サーバ装置において、前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段と、前記ユーザに対してユーザＩＤおよびパスワードを発行する発行手段と、前記認証サーバにおいて前記ユーザＩＤおよび前記パスワードが認証され、ＩＰアドレスを割り当てられた前記ユーザに対して、当該ＩＰアドレスと、前記アプリケーション種別情報と、前記データ方向情報とを対応付けて格納するユーザ情報格納手段と、前記ユーザ情報格納手段によって格納された当該ＩＰアドレスと、前記アプリケーション種別情報と、前記データ方向情報とを前記中継装置に対して送信するユーザ情報送信手段とを備え、前記中継装置において、前記ユーザが送受信する前記データが前記アプリケーション種別情報および前記データ方向情報に合致するか否かを判定し、合致すると判定された前記データについて送受信を許可することを特徴とする。

【００２３】この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザＩＤおよびパスワードを発行し、認証サーバにおいてユーザＩＤおよびパスワードが認証され、ＩＰアドレスを割り当てられたユーザに対して、ＩＰアドレスと、アプリケーション種別情報と、データ方向情報とを対応付けて格納し、格納されたＩＰアドレスと、アプリケーション種別情報と、データ方向情報とを中継装置に対して送信し、中継装置において、ユーザが送受信するデータがアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータ

について送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をＩＳＰ等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【００２４】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記ユーザが前記インターネットの接続を切断した場合には、割り当てられた前記ＩＰアドレスを無効にするＩＰアドレス無効手段をさらに備えたことを特徴とする。

【００２５】この発明によれば、ユーザがインターネットの接続を切断した場合には、割り当てられた前記ＩＰアドレスを無効にするので、ＩＳＰ等に設定されたユーザの情報を削除することができるようになる。

【００２６】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記契約登録手段によって登録されたアプリケーション種別情報および前記データ方向情報を変更する契約変更手段をさらに備えたことを特徴とする。

【００２７】この発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【００２８】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記契約登録手段は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、前記ユーザ情報格納手段は、前記ユーザの当該ＩＰアドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とをさらに対応付けて格納し、前記ユーザ情報送信手段は、前記ユーザの当該ＩＰアドレスと、前記拒絶アプリケーション種別情報と、前記拒絶データ方向情報とを前記中継装置に対してさらに送信し、前記中継装置において、前記ユーザが送受信する前記データが前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、合致すると判定した場合には、当該データを廃棄することを特徴とする。

【００２９】この発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めＩＳＰ等に登録することができるようになる。

【００３０】つぎの発明にかかるインターネット接続システムの管理サーバ装置は、上記の発明において、前記契約変更手段は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更手段と、登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更手段とをさらに備えたことを特徴とする。

【００３１】この発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【００３２】上記目的を達成するため、この発明にかかるインターネット接続方法は、ユーザの情報端末装置をインターネットに接続するためのインターネット接続システムを用いて実行されるインターネット接続方法において、前記ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、前記ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録工程と、前記ユーザに対してユーザＩＤおよびパスワードを発行する発行工程と、前記ユーザが前記インターネットに接続する際に、当該ユーザの前記情報端末装置から前記ユーザＩＤおよび前記パスワードを受信し、当該ユーザＩＤおよび当該パスワードが前記発行工程によって前記ユーザに発行されたものであるか否かを認証する認証工程と、前記認証工程によって認証された場合には、前記ユーザの前記情報端末装置に対してＩＰアドレスを割り当てるＩＰ割当工程と、前記ユーザが送受信する前記データが前記契約登録工程によって登録されたアプリケーション種別情報および前記データ方向情報に合致するか否かを判定する条件判定工程とを含み、前記条件判定工程によって合致すると判定された前記データについて送受信を許可することを特徴とする。

【００３３】この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザＩＤおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザＩＤおよびパスワードを受信し、ユーザＩＤおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に

対してＩＰアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をＩＳＰ等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【００３４】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記ユーザが前記インターネットの接続を切断した場合には、前記ＩＰ割当工程によって割り当てた前記ＩＰアドレスを無効にするＩＰアドレス無効工程をさらに含むことを特徴とする。

【００３５】この発明によれば、ユーザがインターネットの接続を切断した場合には、ＩＰ割当工程によって割り当てた前記ＩＰアドレスを無効にするので、ＩＳＰ等に設定されたユーザの情報を削除することができるようになる。

【００３６】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記契約登録工程によって登録された前記アプリケーション種別情報および前記データ方向情報を変更する契約変更工程をさらに含むことを特徴とする。

【００３７】この発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【００３８】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記条件判定工程によって合致しないと判定された場合には、前記データについて送受信する前記ユーザの前記情報端末装置に対して警告メッセージを送信する警告メッセージ送信工程をさらに含むことを特徴とする。

【００３９】この発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【００４０】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記契約登録工程は、前記ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、前記ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、前記条件判定工程は、前記ユーザが送受信する前記データが前記契約登録工程にて登録された前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致するか否かを判定し、前記条件判定工程によって前記拒絶アプリケーション種別情報および前記拒絶データ方向情報に合致すると判定した場合には、当該データを廃棄することを特徴とする。

【００４１】この発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めＩＳＰ等に登録することができるようになる。

【００４２】つぎの発明にかかるインターネット接続方法は、上記の発明において、前記契約変更工程は、登録された前記アプリケーション種別情報と前記拒絶アプリケーション種別情報とを相互に変更可能にする種別変更工程と、登録された前記データ方向情報と前記拒絶データ方向情報とを相互に変更可能にする方向変更工程とをさらに含むことを特徴とする。

【００４３】この発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【００４４】つぎの発明にかかるプログラムは、上記の発明のいずれか一つに記載されたインターネット接続方法をコンピュータに実行させるプログラムであり、そのプログラムが機械読み取り可能となり、これによって、上記の発明のいずれか一つの動作をコンピュータによって実行することができる。

【００４５】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるインターネット接続システム、管理サーバ装置、インターネット接続方法およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。

【００４６】実施の形態１．図１は、この発明の実施の形態１であるインターネット接続システムのネットワーク構成を示すブロック図である。図１において、情報端末装置２００は、ＲＡＳ（Ｒｅｍｏｔｅ　Ａｃｃｅｓｓ　Ｓｅｒｖｅｒ）４００を介してＩＳＰ網６００に接続される。ＲＡＳ４００は、ユーザの情報端末装置２００からの接続要求を受け、データをＩＳＰ網６００に中継する。ＩＳＰ網６００には、ユーザＩＤ、パスワードをチェックする認証サーバ装置３００、契約したユーザの

情報を管理する管理サーバ装置１００を含んで構成される。管理サーバ装置１００には、ユーザが契約時に申請したアプリケーション種別やデータ方向等のユーザ情報が格納されている。ＩＳＰ網６００は、中継装置５００を経由してインターネット７００に接続されている。ここで、本実施の形態では、ＲＡＳや中継装置等のようにデータを中継、転送する機器をネットワーク機器と称する。

【００４７】図２は、本発明が適用される管理サーバ装置１００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図２において管理サーバ装置１００は、概略的に、管理サーバ装置１００の全体を統括的に制御するＣＰＵ等の制御部１０２、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部１０４、および、各種のデータベース（ユーザ情報データベース１０６ａ）を格納する記憶部１０６を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、このサーバ装置は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ＩＳＰ網６００に通信可能に接続されている。

【００４８】図２の記憶部１０６に格納される各種のデータベース（ユーザ情報データベース１０６ａ）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【００４９】これら記憶部１０６の各構成要素のうち、ユーザ情報データベース１０６ａは、ユーザに関する情報（ユーザ情報）を格納するユーザ情報格納手段であり、認証サーバにおいてユーザＩＤおよびパスワードが認証され、ＩＰアドレスを割り当てられたユーザに対して、ＩＰアドレスと、アプリケーション種別情報と、データ方向情報とを対応付けて格納するユーザ情報格納手段である。ここで、図７は、ユーザ情報データベース１０６ａに格納されるユーザ情報の一例を示す図である。

【００５０】このユーザ情報データベース１０６ａに格納される情報は、図７に示すように、各ユーザを一意に識別するためのユーザ名（ユーザＩＤ）４０、ユーザに割り当てられる割り当てＩＰアドレス４１、ユーザが使用するアプリケーション種別に関するアプリケーション種別情報４２、ユーザが送受信するデータの方向に関するデータ方向情報４３、ユーザがアプリケーションの使用やデータ送受信を許可するかまたは拒絶するかを指定するフラグ４４等から構成される。

【００５１】また、その他の情報として、管理サーバ装置１００の記憶部１０６には、ウェブサイトを情報端末装置２００に提供するための各種のＷｅｂデータやＣＧＩプログラム等が記録されている。

【００５２】このＷｅｂデータとしては、後述する各種のＷｅｂページを表示するためのデータ等があり、これらデータは、例えば、ＨＴＭＬやＸＭＬにて記述されたテキストファイルとして形成されている。また、これらのＷｅｂデータを作成するための部品用のファイルや作業用のファイルやその他一時的なファイル等も記憶部１０６に記憶される。

【００５３】この他、必要に応じて、情報端末装置２００に送信するための音声をＷＡＶＥ形式やＡＩＦＦ形式の如き音声ファイルで格納したり、静止画や動画をＪＰＥＧ形式やＭＰＥＧ２形式の如き画像ファイルで格納したりすることができる。

【００５４】また、図２において、通信制御インターフェース部１０４は、管理サーバ装置１００とＩＳＰ網６００（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部１０４は、他の端末と通信回線を介してデータを通信する機能を有する。

【００５５】また、図２において、制御部１０２は、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部１０２は、機能概念的に、契約登録部１０２ａ、契約変更部１０２ｂ、ＩＤ・パスワード発行部１０２ｃ、ＩＰアドレス無効部１０２ｄ、および、ユーザ情報送信部１０２ｅを備えて構成されている。

【００５６】このうち、契約登録部１０２ａは、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録する契約登録手段である。また、契約変更部１０２ｂは、契約登録手段によって登録されたアプリケーション種別情報およびデータ方向情報を変更する契約変更手段である。また、ＩＤ・パスワード発行部１０２ｃは、ユーザに対してユーザＩＤおよびパスワードを発行する発行手段である。

【００５７】また、ＩＰアドレス無効部１０２ｄは、ユーザがインターネットの接続を切断した場合には、割り当てたＩＰアドレスを無効にするＩＰアドレス無効手段である。また、ユーザ情報送信部１０２ｅは、ユーザ情報格納手段によって格納されたＩＰアドレスと、アプリケーション種別情報と、データ方向情報とを中継装置に対して送信するユーザ情報送信手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【００５８】また、図３は、本発明が適用される認証サーバ装置３００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示し

ている。図３において認証サーバ装置３００は、概略的に、認証サーバ装置３００の全体を統括的に制御するＣＰＵ等の制御部３０２、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部３０４、および、各種のデータベース（ユーザ認証情報データベース３０６ａおよびＩＰアドレス情報データベース３０６ｂ）を格納する記憶部３０６を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、このサーバ装置は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ＩＳＰ網６００に通信可能に接続されている。

【００５９】図３の記憶部３０６に格納される各種のデータベース（ユーザ認証情報データベース３０６ａおよびＩＰアドレス情報データベース３０６ｂ）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【００６０】これら記憶部３０６の各構成要素のうち、ユーザ認証情報データベース３０６ａは、ユーザ認証に関する情報（ユーザ認証情報）を格納するユーザ認証情報格納手段である。このユーザ認証情報データベース３０６ａに格納される情報は、各ユーザを一意に識別するためのユーザＩＤ、および、パスワードから構成される。

【００６１】また、ＩＰアドレス情報データベース３０６ｂは、システム内で利用可能なＩＰアドレスの利用状況を管理するＩＰアドレス情報を格納するＩＰアドレス情報格納手段である。このＩＰアドレス情報データベース３０６ｂに格納される情報は、ＩＰアドレスと、当該ＩＰアドレスを使用しているユーザのユーザＩＤから構成される。

【００６２】また、図３において、通信制御インターフェース部３０４は、認証サーバ装置３００とＩＳＰ網６００（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部３０４は、他の端末と通信回線を介してデータを通信する機能を有する。

【００６３】また、図３において、制御部３０２は、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部３０２は、機能概念的に、ユーザ認証部３０２ａ、および、ＩＰアドレス割当部３０２ｂを備えて構成されている。

【００６４】このうち、ユーザ認証部３０２ａは、ユーザがインターネットに接続する際に、ユーザの情報端末装置からユーザＩＤおよびパスワードを受信し、ユーザＩＤおよびパスワードが発行手段によってユーザに発行されたものであるか否かを認証する認証手段である。また、ＩＰアドレス割当部３０２ｂは、認証手段によって認証された場合には、ユーザの情報端末装置に対してＩＰアドレスを割り当てるＩＰ割当手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【００６５】また、図４は、本発明が適用される中継装置５００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図４において中継装置５００は、概略的に、中継装置５００の全体を統括的に制御するＣＰＵ等の制御部５０２、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部５０４、および、各種のデータベース（ユーザ情報データベース５０６ａ）を格納する記憶部５０６を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、このサーバ装置は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介して、ＩＳＰ網６００またはインターネット７００に通信可能に接続されている。

【００６６】図４の記憶部５０６に格納される各種のデータベース（ユーザ情報データベース５０６ａ）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【００６７】記憶部５０６の各構成要素のうち、ユーザ情報データベース５０６ａは、管理サーバ装置１００から送信されたユーザ情報格納手段であり、ユーザ情報データベース１０６ａと同一の内容が格納されている。

【００６８】また、図４において、通信制御インターフェース部５０４は、中継装置５００とＩＳＰ網６００またはインターネット７００（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部５０４は、他の端末と通信回線を介してデータを通信する機能を有する。

【００６９】また、図４において、制御部５０２は、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部５０２は、機能概念的に、データ受信部５０２ａ、ユーザ特定部５０２ｂ、条件判定部５０２ｃ、データ送信部５０２ｄ、警告メッセージ送信部５０２ｅ、および、ユーザ情報更新部５０２ｆを備えて構成されている。

【００７０】このうち、データ受信部５０２ａは、ユーザが送受信するデータを受信するデータ受信手段である。また、ユーザ特定部５０２ｂは、送受信するデータ

の宛先または送信元のＩＰアドレスから送受信するユーザを特定するユーザ特定手段である。また、条件判定部５０２ｃは、ユーザが送受信するデータが契約登録手段によって登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定する条件判定手段である。

【００７１】また、データ送信部５０２ｄは、条件判定手段によって許可された条件に合致する（または拒絶された条件に合致しない）と判定されたデータについてデータを送信するデータ送信手段である。また、警告メッセージ送信部５０２ｅは、条件判定手段によって許可された条件に合致しない（または拒絶された条件に合致する）と判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信する警告メッセージ送信手段である。また、ユーザ情報更新部５０２ｆは、管理サーバ装置１００から受信したユーザ情報に基づいてユーザ情報データベース５０６ａを更新するユーザ情報更新手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【００７２】また、図５は、本発明が適用される情報端末装置２００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。この図５に示すように、情報端末装置２００は、概略的には、制御部２１０、ＲＯＭ２２０、ＨＤ２３０、ＲＡＭ２４０、入力装置２５０、出力装置２６０、入出力制御ＩＦ２７０、および、通信制御ＩＦ２８０を備えて構成されており、これら各部がバスを介してデータ通信可能に接続されている。

【００７３】この情報端末装置２００の制御部２１０は、Ｗｅｂブラウザ２１１および電子メーラ２１２を備えて構成されている。このうち、Ｗｅｂブラウザ２１１は、基本的には、Ｗｅｂデータを解釈して、後述するモニタ２６１に表示させる表示制御（ブラウズ処理）を行うものである。また、電子メーラ２１２は、所定の通信規約（例えば、ＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ））に従って、電子メールの送受信を行う。

【００７４】また、入力装置２５０としては、キーボード、マウス、および、マイク等を用いることができる。また、後述するモニタ２６１も、マウスと協働してポインティングデバイス機能を実現する。

【００７５】また、出力装置２６０としては、モニタ（家庭用テレビを含む）２６１、および、プリンタ２６２が設けられている。この他、出力装置２６０としては、スピーカ等を用いることができる。出力装置２６０は、通信制御ＩＦ２８０を介して受信された情報を出力する出力手段である。

【００７６】また、通信制御ＩＦ２８０は、情報端末装置２００とネットワーク（またはルータ等の通信装置）との間における通信制御を行う。この通信制御ＩＦ２８０は、管理サーバ装置１００から送信された情報を受信する受信手段である。

【００７７】このように構成された情報端末装置２００は、モデム、ＴＡ、ルータ等の通信装置と電話回線を介して、あるいは、専用線を介して、ネットワークに接続されており、所定の通信規約（たとえば、ＴＣＰ／ＩＰインターネットプロトコル）に従ってＲＡＳ４００にアクセスすることができる。

【００７８】次に、このように構成された本実施の形態における本システムの処理の一例について、以下に図６～図８を参照して詳細に説明する。図６は、本実施形態における本システムを用いて、ユーザがインターネットサービスを利用する際の動作の一例を示すフローチャートである。

【００７９】まず、ユーザは、インターネットサービスを利用するにあたり、ＩＳＰ等のユーザに対してインターネット接続サービスを提供するインターネット接続システムと契約を行う。すなわち、ユーザは、契約時に住所、氏名、電話番号を通知すると共に、例えば、電子メールやホームページ参照等のユーザが使用するアプリケーション種別、ユーザが送受信するデータ方向、および、このアプリケーション種別やデータ方向を許可するか拒絶するかを指定するためのフラグからなるユーザ情報をＩＳＰに通知する（ステップＳＡ－１）。ＩＳＰは、管理サーバ装置１００の契約登録部１０２ａの処理により、通知されたこれらの情報をユーザ情報データベース１０６ａに登録する。

【００８０】ここで、図７は、ユーザ名（ユーザＩＤ）としてｎｅｋｏを指定し、アプリケーション種別としてＥ－ｍａｉｌを指定し、データ方向としてユーザからインターネットを指定し、フラグとして許可を指定し、また、アプリケーション種別としてホームページ閲覧を指定し、データ方向としてユーザからインターネットを指定し、フラグとして拒絶をユーザ情報に指定した場合の管理サーバ装置１００のユーザ情報データベース１０６ａに格納される情報の一例である。

【００８１】なお、ＩＳＰが、インターネット初心者ユーザに対して、お薦めメニューとしてアプリケーション種別（Ｅ－ｍａｉｌ、ＷＷＷ等）、データ方向（ユーザからインターネットへ、または、インターネットからユーザへ）、フラグ（許可、拒絶）を表示するメニュー画面を用意し、ユーザの情報端末装置２００に表示させてもよい。これにより、初心者ユーザも安心して本システムを利用することができるようになる。

【００８２】ついで、ＩＳＰは、管理サーバ装置１００のＩＤ・パスワード発行部１０２ｃの処理により、ユーザに対してインターネット接続で使用するユーザＩＤ、パスワードを発行し、認証サーバ装置３００のユーザ認証情報データベース３０６ａにこれらのユーザ認証情報を登録する（ステップＳＡ－２）。

【００８３】ついで、ユーザは、インターネットサービス利用時にＲＡＳ４００に接続し、ＩＤ、パスワードを通知する（ステップＳＡ－３）。

【００８４】ついで、認証サーバ装置３００は、ユーザ認証部３０２ａの処理により、通知されたＩＤ、パスワードをユーザ認証情報データベース３０６ａにアクセスして検証し、不正な場合は接続を遮断する。一方、正しい場合には、ＩＰアドレス割当部３０２ｂの処理により、ＩＰアドレス情報データベース３０６ｂの中に保持している使用可能なＩＰアドレスの中から１つを選び、このユーザに割り当てる（ステップＳＡ－４）。

【００８５】認証サーバ装置３００は、ユーザに割り当てたＩＰアドレスを管理サーバ装置１００に対して通知し、管理サーバ装置１００では、該通知された割り当てＩＰアドレスをユーザ情報データベース１０６ａに登録する。

【００８６】ついで、管理サーバ装置１００は、ユーザ情報送信部１０２ｅの処理により、ユーザ情報データベース１０６ａに格納されたユーザ情報を中継装置５００に対して配送する。

【００８７】ついで、ユーザがデータをＩＳＰに対して送信すると（ステップＳＡ－５）、中継装置が該データを受信し、図８で示される処理が実行される。図８は、データ受信時の中継装置５００の動作の一例を示すフローチャートである。

【００８８】ここで、中継装置５００におけるデータ受信は、ユーザがインターネットに対して送信したデータ、または、インターネット側から受信したデータの両方のデータに対して行われる。

【００８９】まず、中継装置５００は、データ受信部５０２ａの処理により、データを受信すると（ステップＳＢ－１）、ユーザ特定部５０２ｂの処理により、受信データの送信元あるいは宛先アドレスからユーザを特定する（ステップＳＢ－２）。

【００９０】次に、中継装置５００は、条件判定部５０２ｃの処理により、特定したユーザについてユーザ情報データベース５０６ａを参照して、取得したアプリケーション種別、通信方向、および、フラグの各条件が、受信したデータと合致するかをチェックする（ステップＳＢ－３）。

【００９１】ここで、中継装置５００は、条件が一致する場合（すなわち、許可された条件に合致するか、または拒絶された条件に合致しない場合）には、データ送信部５０２ｄの処理によりデータを送信し（ステップＳＢ－４）、一方、条件が一致しない場合（すなわち、許可された条件に合致しないか、または拒絶された条件に合致する場合）には、警告メッセージ送信部５０２ｅの処理により、データを廃棄し、予め契約登録した以外のデータを受信したことを警告メッセージとしてユーザに通知する（ステップＳＢ－５）。

【００９２】上記の例のように、ユーザが指定したアプリケーション条件に一致したものを送信し、その他をすべて廃棄してもよく、また、条件に一致したものを廃棄し、その他のデータを送信してもよい。

【００９３】再び、図６に戻り、中継装置５００の処理により、予めユーザが契約登録した条件に合致するデータのみが送受信される（ステップＳＡ－６～ステップＳＡ－８）。

【００９４】最後に、ユーザがインターネット接続を切断した場合には、ＲＡＳ４００がこれを検知し、管理サーバ装置１００に通知する。

【００９５】管理サーバ装置１００は、ＩＰアドレス無効部１０２ｄの処理により、ユーザ情報データベース１０６ａに格納されたユーザ情報内のＩＰアドレスを無効にし、また、ユーザ情報送信部１０２ｅの処理により、その旨を中継装置５００に通知する。中継装置５００では、ユーザ情報更新部５０２ｆの処理により、対応するユーザ情報データベース５０６ａのユーザ情報が削除される（ステップＳＡ－９）。

【００９６】以上により、ユーザ側で個々にセキュリティ機器を導入することなく、安全なインターネットサービスを提供できる。また、典型的なメニューを用意することでセキュリティ知識のないユーザや初心者ユーザも安全にインターネットを利用することが可能となる。

【００９７】本実施の形態では、ユーザがＲＡＳに接続する構成を示したが、ＲＡＳの代わりにＡＤＳＬモデムを用いるような常時接続形態も可能である。

【００９８】実施の形態２．つぎに、この発明の実施の形態２について説明する。本実施の形態２では、新たなアプリケーションとしてネットワークゲームを行う場合のように、契約登録したアプリケーション種別をユーザが変更する場合の動作を説明する。図９は、実施の形態２である本システムの動作の一例を示すフローチャートである。なお、ネットワーク構成および各装置の構成は、実施の形態１において図１～図５で示したものと同様である。

【００９９】まず、ユーザは、ユーザＩＤ、パスワードを入力して（ステップＳＣ－１）、情報端末装置２００からＩＳＰ網６００に送信すると（ステップＳＣ－２）、認証サーバ装置３００は、ユーザ認証部３０２ａの処理により、ユーザＩＤ、パスワードをチェックする（ステップＳＣ－３）。

【０１００】そして、チェックがＯＫであれば、管理サーバ装置１００は、契約変更部１０２ｂの処理により、ユーザ情報データベース１０６ａに格納されたユーザ情報のアプリケーション種別情報、データ方向情報、または、フラグの変更をユーザに許容する（ステップＳＣ－４）。

【０１０１】これにより、ユーザは、登録されたアプリケーション種別情報およびデータ方向情報を変更するこ

とができ、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【０１０２】また、契約変更部１０２ｂは、フラグをユーザに変更させることにより、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、また、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にすることもできるので、ユーザは、使用を許可または拒絶するアプリケーションやデータ方向を臨機応変に選択することができるようになる。

【０１０３】ついで、管理サーバ装置１００は、契約変更部１０２ｂの処理により、ユーザの変更結果によりユーザ情報データベース１０６ａを更新した後、ユーザ情報送信部１０２ｅの処理により、該ユーザ情報を中継装置５００に対して配信する（ステップＳＣ－５）。

【０１０４】一方、ステップＳＣ－３においてチェック結果がＮＧの場合は、管理サーバ装置１００は、エラー情報をユーザの情報端末装置２００に表示し（ステップＳＣ－６）、処理を終了する。以上により、ユーザは申請した使用するアプリケーションを安全に変更できる。また、これにより、新たなアプリケーションを使用したい場合にも容易に対応できる。

【０１０５】さて、これまで本発明の実施の形態について説明したが、本発明は、上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてよいものである。

【０１０６】また、実施の形態において説明した各処理のうち、自動的に行なわれるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行なわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種の登録データや検索条件等のパラメータを含む情報、画面例、データベース構成については、特記する場合を除いて任意に変更することができる。

【０１０７】また、管理サーバ装置１００に関して、図示の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。例えば、管理サーバ装置１００、認証サーバ装置３００、ＲＡＳ４００、中継装置５００の各サーバ等が備える処理機能、特に制御部にて行なわれる各処理機能については、その全部または任意の一部を、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）および当該ＣＰＵにて解釈実行されるプログラムにて実現することができ、あるいは、ワイヤードロジックによるハードウェアとして実現することも可能である。

【０１０８】なお、プログラムは、後述する記録媒体に記録されており、必要に応じて管理サーバ装置１００、認証サーバ装置３００、ＲＡＳ４００、中継装置５００に機械的に読み取られる。

【０１０９】また、管理サーバ装置１００、認証サーバ装置３００、ＲＡＳ４００、中継装置５００は、さらなる構成要素として、マウス等の各種ポインティングデバイスやキーボードやイメージスキャナやデジタイザ等から成る入力装置（図示せず）、入力データのモニタに用いる表示装置（図示せず）、システムクロックを発生させるクロック発生部（図示せず）、および、各種処理結果その他のデータを出力するプリンタ等の出力装置（図示せず）を備えてもよい。

【０１１０】また、入力装置、表示装置および出力装置は、それぞれ入出力インターフェースを介して制御部に接続されてもよい。

【０１１１】記憶部に格納される各種のデータベースは、ＲＡＭ、ＲＯＭ等のメモリ装置、ハードディスク等の固定ディスク装置、フレキシブルディスク、光ディスク等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【０１１２】また、管理サーバ装置１００、認証サーバ装置３００、ＲＡＳ４００、中継装置５００は、既知のパーソナルコンピュータ、ワークステーション等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の周辺装置を接続し、該情報処理装置に本発明の方法を実現させるソフトウェア（プログラム、データ等を含む）を実装することにより実現してもよい。

【０１１３】さらに、管理サーバ装置１００、認証サーバ装置３００、ＲＡＳ４００、中継装置５００の分散・統合の具合的形態は図示のものに限られず、その全部または一部を、各種の負荷等に応じた任意の単位で、機能的または物理的に分散・統合して構成することができる。

【０１１４】例えば、各データベースを独立したデータベース装置として独立に構成してもよく、また、処理の一部をＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）を用いて実現してもよい。

【０１１５】また、ＩＰアドレス割当部３０２ｂをＤＨＣＰサーバ（図示せず）により実行してもよい。

【０１１６】また、情報端末装置２００は、既知のパーソナルコンピュータ、ワークステーション、家庭用ゲーム装置、インターネットＴＶ、情報家電装置、ＰＨＳ端末、携帯電話端末、移動体通信端末またはＰＤＡ等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の周辺装置を必要に応じて接続し、該情報処理装置にウェブ情報のブラウジング機能や電子メール機能を実現させるソフトウェア（プログラム、データ等を含む）を実装することにより実現してもよい。

【０１１７】この情報端末装置２００の制御部は、その全部または任意の一部を、ＣＰＵおよび当該ＣＰＵにて解釈実行されるプログラムにて実現することができる。

すなわち、ＲＯＭまたはＨＤには、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）と協働してＣＰＵに命令を与え、各種処理を行うためのコンピュータプログラムが記録されている。このコンピュータプログラムは、ＲＡＭにロードされることによって実行され、ＣＰＵと協働して制御部を構成する。

【０１１８】しかしながら、このコンピュータプログラムは、情報端末装置２００に対して任意のネットワークを介して接続されたアプリケーションプログラムサーバに記録されてもよく、必要に応じてその全部または一部をダウンロードすることも可能である。あるいは、各制御部の全部または任意の一部を、ワイヤードロジック等によるハードウェアとして実現することも可能である。

【０１１９】また、本発明にかかるプログラムを、コンピュータ読み取り可能な記録媒体に格納することもできる。ここで、この「記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等の任意の「可搬用の物理媒体」や、各種コンピュータシステムに内蔵されるＲＯＭ、ＲＡＭ、ＨＤ等の任意の「固定用の物理媒体」、あるいは、ＬＡＮ、ＷＡＮ、インターネットに代表されるネットワークを介してプログラムを送信する場合の通信回線や搬送波のように、短期にプログラムを保持する「通信媒体」を含むものとする。

【０１２０】また、「プログラム」とは、任意の言語や記述方法にて記述されたデータ処理方法であり、ソースコードやバイナリコード等の形式を問わない。なお、「プログラム」は必ずしも単一的に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）に代表される別個のプログラムと協働してその機能を達成するものをも含む。なお、実施の形態に示した各装置において記録媒体を読み取るための具体的な構成、読み取り手順、あるいは、読み取り後のインストール手順等については、周知の構成や手順を用いることができる。

【０１２１】また、ＩＳＰ網６００は、例えば、ＬＡＮ（有線／無線の双方を含む）や、ＶＡＮや、パソコン通信網や、公衆電話網（アナログ／デジタルの双方を含む）や、専用回線網（アナログ／デジタルの双方を含む）や、ＣＡＴＶ網や、ＩＭＴ２０００方式、ＧＳＭ方式またはＰＤＣ／ＰＤＣ－Ｐ方式等の携帯回線交換網／携帯パケット交換網や、無線呼出網や、Ｂｌｕｅｔｏｏｔｈ等の局所無線網や、ＰＨＳ網や、ＣＳ、ＢＳまたはＩＳＤＢ等の衛星通信網等のうちいずれかを含んでもよい。すなわち、本システムは、有線・無線を問わず任意のネットワークを介して、各種データを送受信することができる。

【０１２２】

【発明の効果】以上説明したように、この発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザＩＤおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザＩＤおよびパスワードを受信し、ユーザＩＤおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に対してＩＰアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をＩＳＰ等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【０１２３】つぎの発明によれば、ユーザがインターネットの接続を切断した場合には、ＩＰ割当手段によって割り当てた前記ＩＰアドレスを無効にするので、ＩＳＰ等に設定されたユーザの情報を削除することができるようになる。

【０１２４】つぎの発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【０１２５】つぎの発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【０１２６】つぎの発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めＩＳＰ等に登録することができるようになる。

【０１２７】つぎの発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶

データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【０１２８】つぎの発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザＩＤおよびパスワードを発行し、認証サーバにおいてユーザＩＤおよびパスワードが認証され、ＩＰアドレスを割り当てられたユーザに対して、ＩＰアドレスと、アプリケーション種別情報と、データ方向情報とを対応付けて格納し、格納されたＩＰアドレスと、アプリケーション種別情報と、データ方向情報とを中継装置に対して送信し、中継装置において、ユーザが送受信するデータがアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をＩＳＰ等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【０１２９】つぎの発明によれば、ユーザがインターネットの接続を切断した場合には、ＩＰ割当手段によって割り当てた前記ＩＰアドレスを無効にするので、ＩＳＰ等に設定されたユーザの情報を削除することができるようになる。

【０１３０】つぎの発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【０１３１】つぎの発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めＩＳＰ等に登録することができるようになる。

【０１３２】つぎの発明によれば、登録されたアプリケーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【０１３３】つぎの発明によれば、ユーザが使用を許可するアプリケーションの種別に関するアプリケーション種別情報、および、ユーザが送受信を許可するデータの方向に関するデータ方向情報を登録し、ユーザに対してユーザＩＤおよびパスワードを発行し、ユーザが前記インターネットに接続する際に、ユーザの情報端末装置からユーザＩＤおよびパスワードを受信し、ユーザＩＤおよびパスワードがユーザに発行されたものであるか否かを認証し、認証された場合には、ユーザの情報端末装置に対してＩＰアドレスを割り当て、ユーザが送受信するデータが登録されたアプリケーション種別情報およびデータ方向情報に合致するか否かを判定し、合致すると判定されたデータについて送受信を許可するので、ユーザ個々にファイアウォール等の機材を導入することなく、セキュリティ知識のないユーザに対して安全なインターネット接続サービスを提供することができる。すなわち、ユーザは使用するアプリケーション種別とデータ方向をＩＳＰ等に予め登録することにより、インターネットからユーザの情報端末装置への不正アクセスや、情報端末装置からインターネットへの不用意なデータ流出の可能性を低下させることができる。

【０１３４】つぎの発明によれば、ユーザがインターネットの接続を切断した場合には、ＩＰ割当工程によって割り当てた前記ＩＰアドレスを無効にするので、ＩＳＰ等に設定されたユーザの情報を削除することができるようになる。

【０１３５】つぎの発明によれば、登録されたアプリケーション種別情報および前記データ方向情報を変更するので、ユーザは、使用を許可するアプリケーションやデータ方向を随時変更することができるようになる。

【０１３６】つぎの発明によれば、条件判定によって合致しないと判定された場合には、データについて送受信するユーザの情報端末装置に対して警告メッセージを送信するので、拒絶されたアプリケーションやデータ方向等をユーザに通知することができるようになる。

【０１３７】つぎの発明によれば、ユーザが使用を拒絶するアプリケーションの種別に関する拒絶アプリケーション種別情報、および、ユーザが送受信を拒絶するデータの方向に関する拒絶データ方向情報をさらに登録し、ユーザが送受信するデータが登録された拒絶アプリケーション種別情報および拒絶データ方向情報に合致するか否かを判定し、条件判定によって拒絶アプリケーション種別情報および拒絶データ方向情報に合致すると判定した場合には、データを廃棄するので、ユーザは使用を拒絶するアプリケーションやデータの送受信を拒絶するデータ方向を予めＩＳＰ等に登録することができるようになる。

【０１３８】つぎの発明によれば、登録されたアプリケ

ーション種別情報と拒絶アプリケーション種別情報とを相互に変更可能にし、登録されたデータ方向情報と拒絶データ方向情報とを相互に変更可能にするので、ユーザは、臨機応変に使用を許可または拒絶するアプリケーションやデータ方向を選択することができるようになる。

【０１３９】つぎの発明によれば、上記の発明のいずれか一つに記載されたインターネット接続方法をコンピュータに実行させるプログラムとし、そのプログラムが機械読み取り可能となり、これによって、上記の発明のいずれか一つの動作をコンピュータによって実行することができるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明の実施の形態１であるインターネット接続システムのネットワーク構成を示すブロック図である。

【図２】　本発明が適用される管理サーバ装置１００の構成の一例を示すブロック図である。

【図３】　本発明が適用される認証サーバ装置３００の構成の一例を示すブロック図である。

【図４】　本発明が適用される中継装置５００の構成の一例を示すブロック図である。

【図５】　本発明が適用される情報端末装置２００の構成の一例を示すブロック図である。

【図６】　本実施形態における本システムを用いて、ユーザがインターネットサービスを利用する際の動作の一例を示すフローチャートである。

【図７】　ユーザ情報データベース１０６ａに格納されるユーザ情報の一例を示す図である。

【図８】　データ受信時の中継装置５００の動作の一例を示すフローチャートである。

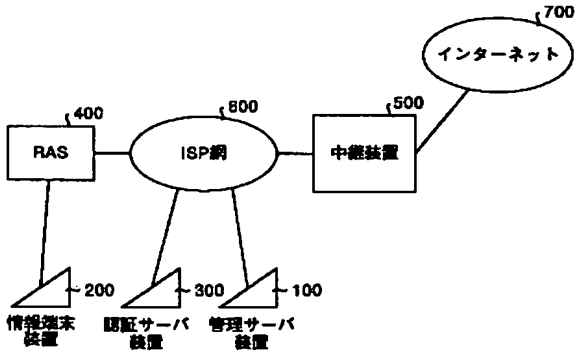
【図９】　実施の形態２である本システムの動作の一例を示すフローチャートである。

【図１０】　従来技術におけるファイアウォールが接続されたネットワーク構成図である。

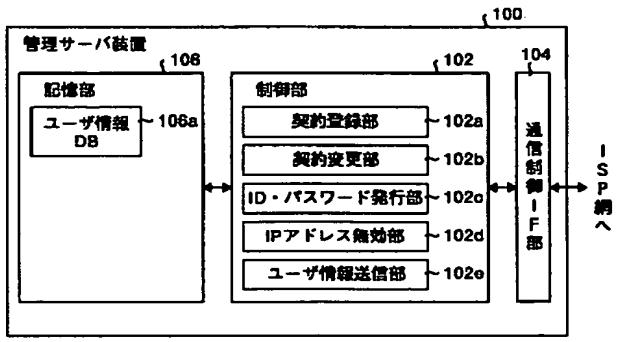
【符号の説明】

４０　ユーザ名、４１　割り当てＩＰアドレス、４２　アプリケーション種別情報、４３　データ方向情報、４４　フラグ、６０　組織内ネットワーク１、６１　組織内ネットワーク２、６２　組織内ネットワーク３、６３　組織ネットワーク、６４　ルータ、６５　インターネット、６６　ＩＳＰ、６７　端末、１００　管理サーバ装置、１０２　記憶部、１０２ａ　契約登録部、１０２ｂ　契約変更部、１０２ｃ　ＩＤ・パスワード発行部、１０２ｄ　ＩＰアドレス無効部、１０２ｅ　ユーザ情報送信部、１０４　通信制御インターフェース部、１０６　記憶部、１０６ａ　ユーザ情報データベース、２００　情報端末装置、２１０制御部、２１１　Ｗｅｂブラウザ、２１２　電子メーラ、２２０　ＲＯＭ、２３０　ＨＤ、２４０　ＲＡＭ、２５０　入力装置、２６０　出力装置、２７０　入出力制御インターフェース、２８０　通信制御インターフェース、３００　認証サーバ装置、３０２　制御部、３０２ａ　ユーザ認証部、３０２ｂ　ＩＰアドレス割当部、３０４　通信制御インターフェース部、３０６　記憶部、３０６ａユーザ認証情報データベース、３０６ｂ　ＩＰアドレス情報データベース、５００　中継装置、５０２　制御部、５０２ａ　データ受信部、５０２ｂ　ユーザ特定部、５０２ｃ　条件判定部、５０２ｄ　データ送信部、５０２ｅ　警告メッセージ送信部、５０２ｆ　ユーザ情報更新部、５０４　通信制御インターフェース部、５０６　記憶部、５０６ａ　ユーザ情報データベース、６００　ＩＳＰ網、７００　インターネット。

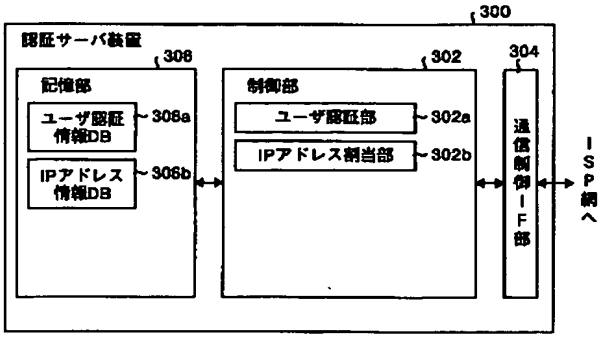
【図１】



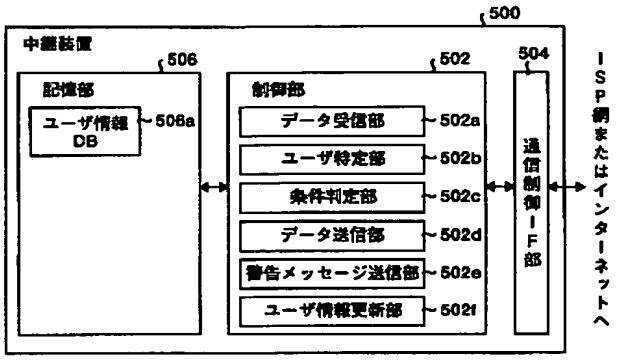
【図２】



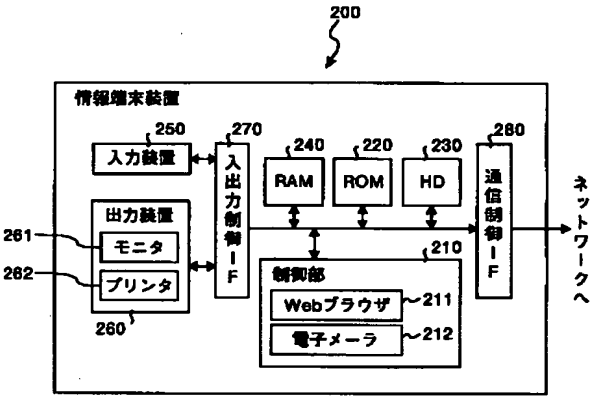
【図３】



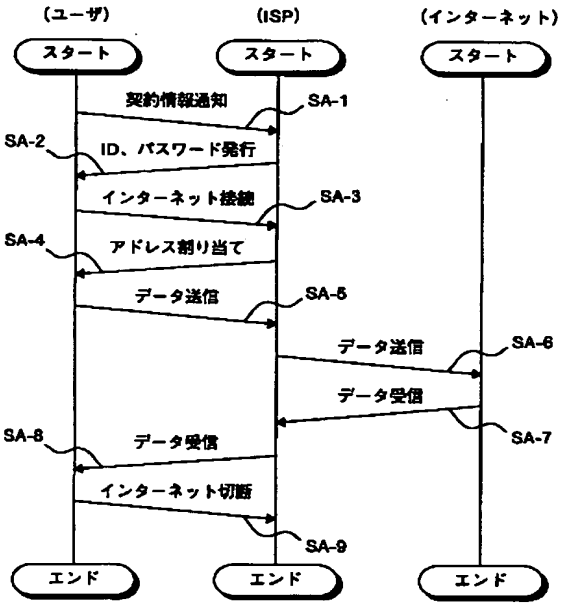
【図４】



【図５】



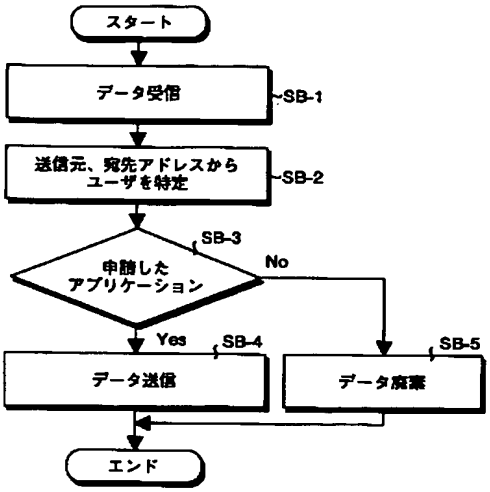
【図６】



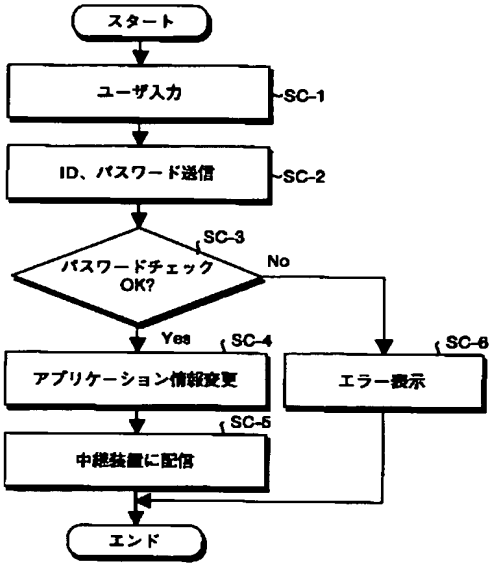
【図７】

40 ユーザ名	41 割り当てIPアドレス	42 アプリケーション種別情報	43 データ方向情報	44 許可/拒絶を指定するフラグ
neko	192.168.0.100	E-mail	ユーザ>インターネット	許可
neko	192.168.0.100	www	ユーザ>インターネット	拒絶
⋮	⋮	⋮	⋮	⋮

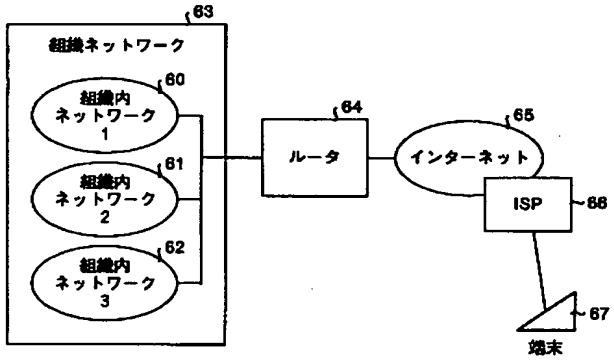
【図８】



【図９】



【図１０】



フロントページの続き

Ｆターム(参考)　5B085 AE01 AE23 BC00 BG07 CA04
5B089 GA11 GA21 GB02 HA10 KA17
5K030 GA15 HB16 HB21 HC01 HC14
HD03 HD08 JA07 JA11 JL07
JT03 JT06 KA06 KA07 KX24
LB02 LC15 LC18 LD19 LD20
MA04 MC08
5K033 AA08 BA04 BA15 CA19 CB09
CC02 DA05 DB14 DB18 DB20
EA02 EA06 EC04